Thema-audit

Beheer van ICT-risico's bij lokale besturen

Globaal rapport | 13.06.2023

Vlaamse overheid

AUDIT VLAANDEREN

AUDIT
VLAANDEREN

INHOUDSOPGAVE

AUDIT
VLAANDEREN

1 SITUERING VAN DE THEMA-AUDIT BEHEER VAN ICT-RISICO'S BIJ LOKALE BESTUREN

Audit Vlaanderen voerde in de periode oktober '21 – maart '22 de thema-audit Beheer van ICT-risico's bij lokale besturen uit bij 144 lokale besturen.

Een beknopter zicht op het beheer van ICT-risico's bij een grote groep andere lokale besturen werd verzameld tussen april '20 en voorjaar '23 via ICT-veiligheidsaudits. Dit zicht bevestigt dat de bevindingen van deze thema-audit in lijn liggen met het globaal beeld voor heel Vlaanderen. Een rapportering over de bevindingen uit de ICT-veiligheidsaudits met cofinanciering in de periode 2020-2022 zal nog midden dit jaar worden gefinaliseerd.

Voor de thema-audit beheer van ICT-risico's werden geen individuele auditrapporten opgemaakt voor elk deelnemend bestuur. Het rapport is zo opgevat dat elk bestuur zelf de eigen zelfevaluatie kan vergelijken met de globale resultaten van de 144 lokale besturen. Het inspiratierapport laat toe om aan de hand van bouwstenen zelf aan de slag te gaan met verbeteracties, ongeacht het startniveau van het lokaal bestuur.

2 GLOBALE CONCLUSIE VAN DE THEMA-AUDIT BEHEER VAN ICT-RISICO'S BIJ LOKALE BESTUREN

De voorbije jaren hebben de lokale besturen vooral onder impuls van de Algemene Verordening Gegevensbescherming (AVG) belangrijke stappen gezet op het vlak van informatieveiligheid. In dit kader werden ook risico's met betrekking tot informatieveiligheid in kaart gebracht. Toch zijn er voor de meeste lokale besturen nog belangrijke verbeterpunten om verder te evolueren richting een breder, meer systematisch beheer van alle ICT-risico's. Een goed uitgebouwd beheer van de belangrijkste ICT-risico's wint steeds meer aan belang omdat veel lokale besturen inzetten op doorgedreven digitalisering van hun processen en hun dienstverlening.

Hoewel 123 van de 144 lokale besturen die deelnamen aan de thema-audit in hun meerjarenplan doelstellingen hebben geformuleerd met betrekking tot digitalisering en ICT, heeft minder dan de helft ook een concreet ICT-actieplan. Slechts een derde van de bevraagde besturen heeft een actuele ICT-risicoanalyse.

Dit betekent dat de randvoorwaarden om proactief aan beheer van de ICT-risico's te doen bij de meeste lokale besturen niet vervuld zijn. Uit de zelfevaluatie van de 144 lokale besturen die aan deze audit deelnamen, blijkt dan ook dat lokale besturen zelf aangeven dat er nog belangrijke werkpunten zijn om bepaalde ICT-risico's voldoende te beheersen.

Eén van deze belangrijke werkpunten heeft betrekking op de samenwerking met externe dienstverleners. Lokale besturen zijn voor hun ICT-projecten en voor het dagdagelijks beheer van de software en de data sterk afhankelijk van externe leveranciers. Deze ontzorging kan een vals gevoel van veiligheid geven. In de praktijk is het vaak onduidelijk welke leverancier bijvoorbeeld instaat voor het beheer van (een bepaald deel van) de ICT-infrastructuur. Het is soms ook onduidelijk waar en door wie de data van het lokaal bestuur wordt beheerd. Lokale besturen maken gebruik van een hele resem van extern ontwikkelde toepassingen (inclusief configuratie in het netwerk, monitoringsmogelijkheden en beveiliging ervan) en hebben daarover weinig overzicht,. Het samenspel tussen de lokale besturen en hun dienstverleners zorgt momenteel in vele gevallen voor een onvoldoende goed beheer van de belangrijkste ICT-risico's.

Een goed werkende ICT-omgeving brengt heel wat taken met zich mee. De ICT-functie blijkt in de praktijk vaak beperkt opgezet in verhouding tot de verwachtingen en doelstellingen. ICT-personeel wordt dikwijls heel operationeel ingezet voor tal van taken zoals het uitbaten van de helpdesk en heeft weinig tijd en mentale ruimte om de dialoog aan te gaan met het managementteam over de ICT-risico's van het lokaal bestuur. In enkele gevallen is de situatie ook op operationeel vlak schrijnend en was de ICT-functie niet ingevuld tijdens de audit. Gecombineerd met onvoldoende documentatie van de ICT is dit een risico op zich. Door de krappe invulling van de interne ICT-functie is er soms geen tijd voor essentiële beheersmaatregelen zoals het tijdig nemen van back-ups en het documenteren van ICT-processen.

3 DANKWOORD

Audit Vlaanderen wil de 144 bevraagde lokale besturen bedanken voor de constructieve samenwerking. In eerste instantie was de bevraging gericht naar de ICT-verantwoordelijke van het lokaal bestuur. In de praktijk namen een aantal lokale besturen zelf het initiatief om ook de algemeen directeur, de DPO (functionaris voor gegevensbescherming) en ook hun externe dienstverleners te betrekken bij het beantwoorden van de vragen. Dit illustreert het belang dat lokale besturen hechten aan het thema “het beheer van ICT-risico’s”. Alle lokale besturen die werden uitgenodigd om deel te nemen, vulden een uitgebreide vragenlijst met een zelfevaluatie in. Dit maakte het mee mogelijk om tot dit globaal rapport te komen.

4 CONCLUSIES VAN DE THEMA-AUDIT BEHEER VAN ICT-RISICO'S BIJ LOKALE BESTUREN

1. **Lokale besturen willen inzetten op ICT en digitalisering, maar pakken dit weinig gestructureerd en concreet aan.**

4.1.1 De meeste lokale besturen hebben digitalisering hoog op de agenda staan

Deze audit ging onder meer na in welke mate lokale besturen **doelstellingen met betrekking tot digitalisering en ICT** hebben vooropgesteld, bijvoorbeeld in het meerjarenplan 2020-2025. Dit is immers een randvoorwaarde om te komen tot een gestructureerde aanpak van digitalisering, van de uitbouw van ICT en van het beheer van ICT-risico's binnen het lokaal bestuur.

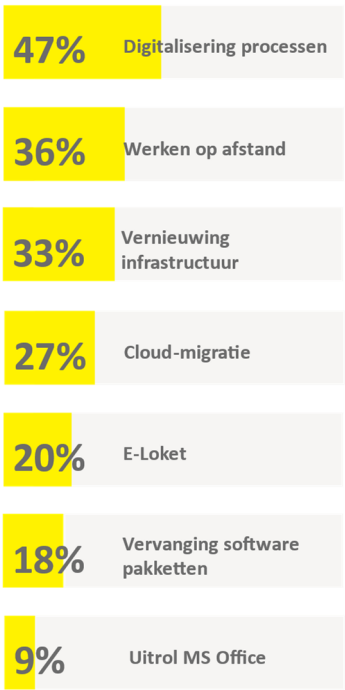
85% van de 144 lokale besturen heeft expliciet doelstellingen m.b.t. ICT en digitalisering vooropgesteld

Uit de antwoorden van de online bevraging blijkt dat 85% (123/144) van de lokale besturen doelstellingen heeft met betrekking tot ICT en digitalisering in het meerjarenplan. Bij 15 van de 21 besturen die dergelijke doelstellingen niet (expliciet) vooropgesteld hebben, maakt de ICT-verantwoordelijke geen deel uit van het managementteam en heeft hij of zij geen mogelijkheid om autonoom agendapunten te agenderen op het managementteam.

De **projecten** die de ICT-functie uitvoert, variëren van het digitaliseren van de processen en de dienstverlening tot de verdere uitbouw van de ICT-infrastructuur en de applicaties. Voor een aantal besturen (40%) zijn hier prioritaire acties in het meerjarenplan aan gekoppeld. De doelstellingen worden meestal niet expliciet geformuleerd als actie. Vaak zitten digitaliseringsdoelstellingen verscholen onder een bredere actie bijvoorbeeld: het verbeteren van de dienstverlening aan de burger. Hierdoor is het niet mogelijk een algemeen overzicht te maken van de doelstellingen die de lokale besturen in Vlaanderen hebben vooropgesteld voor ICT en welke budgetten daaraan gekoppeld zijn.

Tijdens de diepte-interviews met 45 lokale besturen werd gepeild naar het soort projecten waaraan de laatste drie jaren werd gewerkt. De figuur hiernaast geeft weer welk aandeel van de 45 lokale besturen werk maakte of bezig was met een bepaald type project.

In de praktijk zijn er dus veel ambities en wordt er vaak gelijktijdig gewerkt aan verschillende projecten.



4.1.2 Vaak ontbreekt een gevalideerde ICT-visie/-strategie

Uit de online bevraging blijkt dat net iets minder dan de helft van de 144 lokale besturen een ICT-visie/-strategie heeft die ook met het managementteam werd besproken en die formeel is gevalideerd.

46% van de bevraagde lokale besturen heeft een met het management besproken en gevalideerde ICT-visie/-strategie

Een gevalideerde ICT-visie/-strategie is nochtans een belangrijk instrument om volgende risico's in de hand te houden:

- inefficiënte inzet van middelen (geld en personeel) voor de meest prioritaire zaken;
- onvoldoende onderbouwde keuzes met betrekking tot de ICT-structuur, ICT-governance en uitbesteding;
- onvoldoende afbakening van rollen en verantwoordelijkheden;
- meerdere toepassingen die niet op elkaar aansluiten of juist meerdere toepassingen die elkaar overlappen of zouden kunnen worden vervangen door één enkele toepassing;
- onvoldoende aansluiting tussen ICT en de noden van de organisatie.

4.1.3 Een minderheid van de besturen heeft een concreet ICT-actieplan en volgt de uitvoering ervan op

Hoewel de meerderheid van de lokale besturen doelstellingen heeft op het vlak van digitalisering en ICT heeft slechts 40% die doelstellingen ook doorvertaald naar een concreet actieplan.

40% van de bevraagde lokale besturen heeft een concreet actieplan.

Audit Vlaanderen vroeg aan een selectie van 45 van de 144 lokale besturen om de documenten te bezorgen die zij hanteren om de ICT-visie en -strategie vorm te geven en de acties op te volgen. Aan de hand van een inhoudelijke analyse van deze documenten ging Audit Vlaanderen na in welke mate het actieplan aansluit op de doelstellingen op het vlak van digitalisering en ICT in het meerjarenplan. Hierbij werd eveneens nagegaan of het actieplan daadwerkelijk voldoende houvast biedt voor het lokaal bestuur om beslissingen te nemen met betrekking tot de verdere digitalisering van de processen. Via een dieptegesprek met de ICT-verantwoordelijke(n) werd besproken op welke manier het managementteam de acties opvolgt. Ook de manier waarop het managementteam en de ICT-functie samenwerken om de ICT-visie en -strategie te realiseren kwam aan bod.

Op basis van deze documentenanalyse categoriseerde Audit Vlaanderen de 45 deelnemende lokale besturen op een maturiteitsschaal. De resultaten van deze oefening worden weergegeven in volgende figuur:

Maturiteit 4	**11%**	Een gedocumenteerde en onderbouwde visie en een actieplan dat gemonitord wordt.
Maturiteit 3	**9%**	Een gedocumenteerde en onderbouwde visie die een houvast biedt.
Maturiteit 2	**29%**	Een visie die gedeeltelijk houvast biedt en aansluit op de organisatiestrategie maar verspreid zit over verschillende documenten.
Maturiteit 1	**47%**	Een visie die: – beperkt is of geen rekening houdt met technologische evoluties; – niet gedocumenteerd is; – gedeeltelijk aansluit op de organisatiestrategie.
Maturiteit 0	**4%**	Geen ICT-visie of -strategie

Bij iets meer dan de helft (51%) van de 45 lokale besturen is er enkel een heel fragmentaire ICT-visie die niet of slechts gedeeltelijk aansluit op de organisatiestrategie en die onvoldoende rekening houdt met nieuwe trends en technologische evoluties.

Ongeveer een derde van de bevraagde besturen (29%) heeft wel een visie die een zekere houvast biedt, maar de visie en de acties zijn niet vastgelegd in een document ter bekrachtiging en voor verdere communicatie. Gebrekkige of fragmentaire documentatie maakt het dan moeilijk om de voortgang systematisch op te volgen (te monitoren).

Slechts 11% (5/45) van de bevraagde besturen haalt maturiteitsniveau 4 en heeft een coherente en onderbouwde visie voor ICT en digitalisering die ook aansluit op de organisatiedoelstellingen en een concreet actieplan dat ook effectief wordt opgevolgd (gemonitord).

Er kon geen duidelijke correlatie worden vastgesteld tussen het maturiteitsniveau van een lokaal bestuur en de grootte van het lokaal bestuur (volgens het inwonersaantal), de invulling van de ICT-functie (aantal VTE) of de positionering van de ICT-functie in de organisatie. Waarschijnlijk zijn er andere factoren die bepalen of er sprake is van een degelijk ICT-visie/strategie.

2. **Lokale besturen hebben slechts een deel van hun ICT-risico's in het vizier en zij schatten zelf in dat er nog belangrijke werkpunten zijn.**

4.2.1. De verplichtingen ingevolge de AVG hebben het beheer van ICT-risico's gestimuleerd

De meeste lokale besturen hebben de voorbije jaren wel stappen gezet op het vlak van het beheer van de ICT-risico's en dit veelal in het kader van de AVG.
Onder impuls van de DPO-functie (de verplichte functionaris voor gegevensbescherming) hebben de meeste lokale besturen werk gemaakt van een risicoanalyse op het vlak van informatieveiligheid. Dit is opvallend aangezien de DPO het toezicht op de veiligheid van de verwerking van persoonsgegevens beoogt en dus niet verantwoordelijk is voor het uitbouwen van ICT, ICT-risico's en/of ICT-veiligheid.

De mate waarin de DPO met een bredere blik kijkt naar meer algemene ICT-risico's verschilt van bestuur tot bestuur. Ook de bredere risicoanalyses missen vaak nog een aantal thema's, zoals het contractmanagement met ICT-dienstverleners en het beheer van softwarelicenties. De risicoanalyse die werd opgemaakt vertrekt meestal ook niet vanuit de organisatiedoelstellingen en de vooropgestelde ambities op het vlak van digitalisering, maar is gericht op informatieveiligheid en de verwerking van persoonsgegevens.

Alleszins blijkt wel dat de AVG een belangrijke rol heeft gespeeld in de creatie van meer bewustzijn over het belang van het beheer van ICT-risico's bij het management van de lokale besturen. Door de inrichting van de DPO-functie en de organisatie van een informatieveiligheidscel of -overleg groeide ook het inzicht dat er nood is aan afspraken binnen de organisatie, bijvoorbeeld over de verantwoordelijkheden voor bepaalde risico's en het eigenaarschap van acties uit het ICT-actieplan.

Veel lokale besturen gaven aan dat door de AVG ook het inzicht gegroeid is dat ICT-risico's geen loutere technologische aangelegenheid zijn, maar dat ook de manier waarop eindgebruikers omgaan met hardware, software en gegevens een belangrijke risicofactor kan zijn.

4.2.2. De meeste ICT-risico-analyses dekken maar een gedeelte van de ICT-risico's af

Uit de online bevraging blijkt dat 30% van de 144 lokale besturen beschikt over een recente ICT-risicoanalyse (die niet ouder is dan drie jaar). Bijna de helft (49%) heeft slechts een gedeeltelijke risicoanalyse en 21 % heeft geen risicoanalyse of de risicoanalyse is meer dan drie jaar oud.

De meeste lokale besturen die een risicoanalyse hebben gemaakt, hebben dit gedaan in het kader van informatieveiligheid (AVG) of in het kader van de omgevingsanalyse aan het begin van de legislatuur.

4.2.3. Lokale besturen geven aan dat er nog belangrijke werkpunten zijn om ICT-risico's onder controle te brengen

In de online bevraging werd aan de 144 lokale besturen gevraagd om een zelfevaluatie te maken over de maturiteit van 13 risicodomeinen[1] met betrekking tot ICT.
Bij zes risicodomeinen geeft meer dan 50% van de lokale besturen aan dat er nog belangrijke werkpunten zijn.

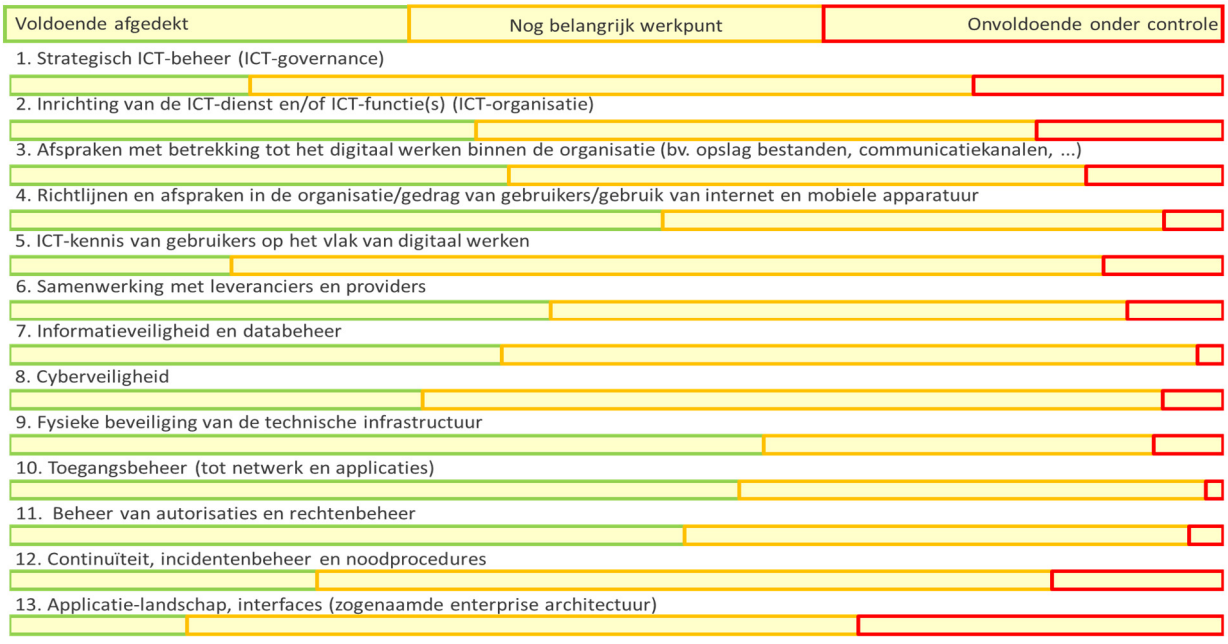
- Strategisch ICT-beheer;
- ICT-kennis van eindgebruikers op het vlak van digitaal werken;
- Informatieveiligheid en databeheer;
- Cyberveiligheid;
- Continuïteit, incidentenbeheer en noodprocedures;
- Applicatielandschap en interfaces.

Tijdens de verdere diepte-interviews werd vaak ook gewezen op risico's die verbonden zijn aan het digitale werken en op het gebrek aan duidelijke afspraken daaromtrent met de eindgebruikers (bv. over dataopslag en digitale communicatie met burgers en bedrijven).

Voor vier risicodomeinen geeft meer dan de helft van de besturen aan dat ze wel voldoende afgedekt zijn:

- Richtlijnen en afspraken in de organisatie/gedrag van eindgebruikers/gebruik van internet en mobiele apparatuur;
- Fysieke beveiliging van de technische infrastructuur;
- Toegangsbeheer (tot netwerk en applicaties);
- Beheer van autorisaties en rechtenbeheer.

Onderstaande figuur geeft het volledige overzicht van de zelfevaluatie van de 13 risicodomeinen van de 144 lokale besturen:



[1] Organisaties worden blootgesteld aan tal van ICT-risico's zoals het kraken van paswoorden, diefstal van gegevens maar bijvoorbeeld ook aan fysieke risico's zoals een brand, overstroming enz. Om risico's beheersbaar en bespreekbaar te maken worden risico's volgens hun aard gecategoriseerd in zogenaamde **risicodomeinen**.

Besturen gaven aan dat er nog heel wat werkpunten zijn, maar dat een heel aantal acties wel al lopende zijn of alleszins nog op de planning stonden.

Aan de hand van een lijst van 20 concrete beheersmaatregelen peilde Audit Vlaanderen bij de 144 lokale besturen naar de maturiteit van de meest voor de hand liggende beheersmaatregelen in de verschillende risicodomeinen.

Onderstaande beheersmaatregelen behaalden lage scores (15-30%) en zijn 'in beperkte mate' of 'helemaal niet' geïmplementeerd.

- De ICT-strategie wordt gedragen/is gekend door het bestuur en de ruimere organisatie.
- In de ICT-dienst is er voldoende kennisoverdracht en er worden vervangers voorzien voor personeelsleden die een kritieke functie uitoefenen.
- Rollen en verantwoordelijkheden binnen de ICT-dienst, alsook ICT-processen werden gedocumenteerd en zijn duidelijk voor de gehele organisatie.
- Er is een gedocumenteerd overzicht van alle bestaande licenties met hun vervaldatum.
- Er is adequate noodplanning/een bedrijfscontinuïteitsplan/een disaster recovery plan aanwezig die ook voorziet in de aanpak van een ICT-incident (vb een cyberaanval).

Volgende beheersmaatregelen werden door de meerderheid (50% of meer) van de 144 lokale besturen aangegeven als 'grotendeels wel' geïmplementeerd.

- We volgen nieuwe technologische evoluties en innovatie in ICT actief op.
- Er wordt rekening gehouden met organisatieveranderingsbeheer om digitalisering te verankeren in de organisatie (vb. invoering digitaal vergaderen).
- Er is een gedocumenteerd overzicht van de hardware (PC's, laptops, servers, displays, automaten,…) van het lokaal bestuur.
- De eindgebruikers maken enkel gebruik van geautoriseerde en gekende systemen bij de ICT-dienst, met andere woorden er wordt geen gebruik gemaakt van schaduwsoftware.
- Er is een goed bewustzijn binnen de organisatie rond informatieveiligheid en cyberveiligheid.

De volledige zelfevaluatie werd in onderstaand overzicht samengevat:

Zelfevaluatie van de maturiteit van de 20 beheersmaatregelen voor de 144 lokale besturen

De opvolging van de samenwerking met verschillende partijen is een beheersmaatregel die voor veel lokale besturen een uitdaging vormt (10).

Opvallend is dat slechts een minderheid van de lokale besturen aangeeft dat zij voldoende documentatie hebben (punt 11, 12, 13 en 20). De combinatie van gebrekkige documentatie van het ICT-hardware, software en processen en de grote afhankelijkheid van externen vormt een groot risico voor veel lokale besturen. Een actueel overzicht van de toepassingen en informatieopslag ontbreekt vaak. In dat geval is het niet duidelijk welke externe partij welke informatie beheert en waar de data van het lokaal bestuur zich fysiek bevindt. Dit bemoeilijkt ook de uitwerking van een adequate noodplanning en een bedrijfscontinuïteitsplan. 15% van de lokale besturen heeft geantwoord dat ze niet beschikken over een adequate noodplanning. 58% geeft aan dat er een gedeeltelijke of beperkte noodplanning voorhanden is. Het is onduidelijk hoe deze besturen de continuïteit van de dienstverlening zullen garanderen indien er zich een incident voordoet (daarbij kan gedacht worden aan externe risico's zoals natuurrampen, cyberaanvallen en problemen met de energievoorziening).

Bij een vijftal besturen waarmee Audit Vlaanderen in gesprek ging was de situatie kritiek met ernstige operationele ICT-risico's tot gevolg (bijvoorbeeld het niet meer maken van back-ups van de gegevens gedurende een langere periode).

3. **Lokale besturen zijn zich onvoldoende bewust van de risico's die verbonden zijn aan hun samenwerking met externe leveranciers.**

4.3.1. Lokale besturen zijn sterk afhankelijk van externe dienstverleners

De meeste lokale besturen zijn afhankelijk van (tal van) externe dienstverleners en leveranciers voor het beheer van hun ICT-infrastructuur en voor hun databeheer.

De 45 lokale besturen gaven aan minstens 10 tot vaak meer dan 20 leveranciers te hebben die applicaties leveren en de data van het lokaal bestuur (gedeeltelijk) beheren.

Het ICT-beheer wordt niet zelden volledig overgelaten aan externen zonder dat er passende overeenkomsten of afspraken zijn met aandacht voor rollen en verantwoordelijkheden op het vlak van risicobeheer. Het is niet altijd duidelijk wie instaat voor de beveiliging en het beheer van bepaalde hardware en software..

Zo is het mogelijk dat bepaalde updates (bijvoorbeeld van een firewall) niet tijdig of zelfs helemaal niet gebeuren waardoor er in feite gaten in de beveiliging ontstaan. Als bepaalde software niet tijdig geüpdatet wordt, ontstaat het risico dat een bepaalde toepassing plots niet meer functioneert.

In de online bevraging geeft 66% van de lokale besturen aan dat "samenwerking met leveranciers en providers" een belangrijk werkpunt is.

De ontzorging geeft vaak een vals gevoel van veiligheid: men schakelt deskundigen in, maar men heeft zelf onvoldoende kennis en expertise om een goede opvolging of aansturing te organiseren van deze uitbesteding.

4.3.2. Een versnipperd landschap van softwaretoepassingen

Lokale besturen kopen hun softwarepakketten bijna uitsluitend extern aan bij verschillende leveranciers. Dit geldt zowel voor softwarepakketten om de kernprocessen en de dienstverlening te ondersteunen als voor ondersteunende software (bv. boekhouding, aankopen, personeelsbeheer, loonadministratie,...).

De laatste jaren ontstond op dit vlak een spanningsveld.
Vanuit beheersbaarheid en efficiëntie lijkt het enerzijds logisch om zoveel mogelijk te kiezen voor pakketten van eenzelfde familie (stack) of van eenzelfde leverancier of voor een geïntegreerde omgeving (zogenaamde ERP-software voor bijvoorbeeld de ondersteunende processen). Anderzijds is er ook een groeiend aanbod van heel specifieke nichesoftware voor lokale besturen (bv. voor het beheer van begraafplaatsen, handhaving op het terrein met mobiele toestellen, ...). Deze software werd specifiek ontwikkeld op maat van een jeugddienst of een technische dienst en speelt heel precies in op de specifieke noden van bepaalde diensten. De generieke componenten in deze toepassingen (online een aanvraag doen, een kaartje van de gemeente raadplegen, online betalen,...) worden in meerdere toepassingen op een verschillende manier aangeboden.

Een aantal ICT-verantwoordelijken maakten tijdens de diepte-interviews de opmerking dat er binnen hun bestuur verschillende applicaties dubbel of zelfs meervoudig geïmplementeerd zijn voor het maken van reservaties en afspraken, voor digitale aanvragen, voor online betalingen enz. Dit maakt het beheer van ICT-risico's complexer.

Er is bijna geen enkel lokaal bestuur dat beschikt over een duidelijk, actueel overzicht van hoe die verschillende applicaties met elkaar geconnecteerd zijn en waar/door wie de data van het lokaal bestuur juist beheerd wordt.

Dit stelt de ICT-functie voor bijzondere uitdagingen. Door de complexiteit van het softwarelandschap, de onduidelijkheid over welke data waar wordt opgeslagen en de ontoereikende documentatie van het ICT-beheer is een actief risicobeheer moeilijk.

4. **De capaciteit en positionering van de ICT-functie sluiten onvoldoende aan bij het benodigde risicobeheer en de ambities op het vlak van digitalisering.**

4.4.1. Een breed takenpakket

Er zijn grote verschillen tussen lokale besturen in de bestaffing van de ICT-functie, maar algemeen blijkt dat de interne capaciteit erg beperkt is en moet instaan voor een breed takenpakket:

- Het uitbaten van de ICT-helpdesk;
- Het dagdagelijks beheer van applicaties en infrastructuur;
- Het installeren van nieuwe hardware en telefonie;
- Het documenteren en het actueel houden van de ICT-architectuur;
- Het opvolgen van ICT-leveranciers;
- Overleg in het kader van informatieveiligheid.

	60% van de 144 lokale besturen voorzien tussen 0,1 en 2 VTE voor hun ICT-dienst.
	Bij 33% van de 144 lokale besturen is het voorziene aantal VTE niet volledig ingevuld.
	7% van de 144 lokale besturen had geen interne ICT-functie tijdens de audit.
	10 van de 144 bevraagde lokale besturen signaleerden ernstige problemen bij de invulling van de interne ICT-functie.

Soms nemen de eigen medewerkers deze taken op. Vaak wordt een beroep gedaan op externe medewerkers die via een dienstverleningsovereenkomst of ad hoc op basis van bv. aanvaarde factuur ondersteuning bieden. Er zijn ook lokale besturen die zelf geen of nauwelijks ICT-kennis in huis hebben.

4.1.4 Beperkte capaciteit van ICT-functie

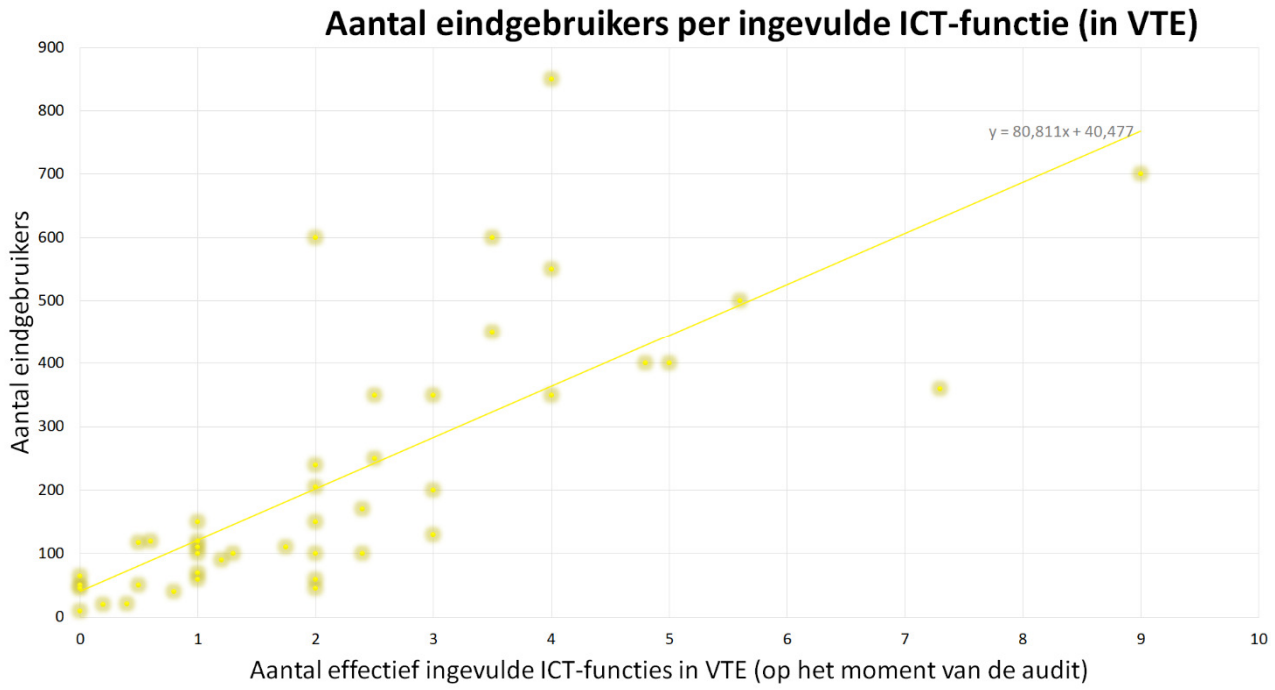
Met de relatief beperkte interne ICT-capaciteit is er bij veel lokale besturen weinig ruimte voor het opstellen van een ICT-strategie en het (strategisch) meedenken met het management en de eindgebruikers over mogelijke oplossingen en innovaties. In deze context is het niet evident om voldoende aandacht te besteden aan het beheer van ICT-risico's.

Tijdens de audit werd nagegaan of er een correlatie is tussen de grootte van het lokaal bestuur (in termen van aantal inwoners), de breedte van het takenpakket voor de eigen ICT-medewerkers en de mate waarin het bestuur taken uitbesteedt, maar geen enkele van deze factoren bleek een correlatie te vertonen met het aantal voorziene interne ICT-functies en de effectieve invulling ervan.

De enige correlerende factor blijkt het aantal eindgebruikers te zijn dat een beroep kan doen op de ICT-dienstverlening van het lokaal bestuur. De eindgebruikers zijn uiteraard de interne personeelsleden van het lokaal bestuur en de mandatarissen, maar in veel gevallen ook verbonden organisaties zoals de personeelsleden van een woonzorgcentrum of een school. Enkele besturen leveren ook ICT-dienstverlening aan externe organisaties zoals bijvoorbeeld de politiezone.

Hoewel bij elk van de 144 lokale besturen werd bevraagd met hoeveel VTE de ICT-functie ingevuld was, waren de antwoorden hierop niet helemaal betrouwbaar. In de diepte-interviews werd dieper ingegaan op de effectieve invulling en het aantal eindgebruikers.

De relatie tussen het aantal effectief ingevulde interne ICT-functies (op het moment van de bevraging) en het aantal bediende eindgebruikers voor de 45 bevraagde besturen die minder dan 10 VTE ICT-functie hadden, wordt weergegeven in onderstaande figuur.



Elk geel punt in bovenstaande figuur is een lokaal bestuur. De trendlijn geeft het verband weer tussen het aantal effectief ingevulde ICT-functies en het aantal eindgebruikers.

Uit deze grafiek kan het volgende worden afgeleid:
- Voor elke 80 bijkomende eindgebruikers wordt er in de praktijk één extra interne ICT medewerker ingeschakeld.
- Bij een aantal kleinere lokale besturen (met minder dan 71 eindgebruikers), bleken er geen interne ICT-medewerkers op de werkvloer aanwezig te zijn tijdens de audit.
- Er is een grote groep van besturen met minder dan 2 VTE ICT-functie. In combinatie met een gebrekkige documentatie van de ICT-architectuur en processen vormt dit een belangrijk risico.

4.4.2. Positie van de ICT-functie in de organisatie

De positie van de ICT-functie in het organigram en de overlegmogelijkheden met het managementteam zijn belangrijke randvoorwaarden om de ICT-visie/-strategie vorm te geven en uit te rollen in heel de organisatie. Uit de diepte-interviews met 45 lokale besturen blijkt dat er bij de besluitvorming door het managementteam vaak onvoldoende rekening wordt gehouden met ICT-aspecten. Een belangrijke oorzaak hiervoor is meestal de positie die de ICT-functie inneemt in de organisatie en meer bepaald de relatie tussen de ICT-functie en het management van de organisatie.

Daarom werd nagegaan in welke mate de ICT-functie toegang heeft tot het managementteam om o.a. ICT-gerelateerde keuzes (beslissingen) te kunnen ondersteunen, toelichting te kunnen geven bij diepgaandere technische aspecten of digitalisering. Bij de 45 geïnterviewde lokale besturen blijkt het volgende :

- in 9% van de lokale besturen maakt de ICT-verantwoordelijke zelf deel uit van het managementteam.
- bij 22% van de lokale besturen kan de ICT-verantwoordelijke autonoom punten agenderen op het managementteam.
- bij 62% worden ICT-punten geagendeerd op het managementteam via de leidinggevende van de ICT-verantwoordelijke of de algemeen directeur.
- 7% van de ICT-verantwoordelijken heeft geen (rechtstreekse of onrechtstreekse) toegang tot het managementteam.

Bij een deel van de lokale besturen wordt de ICT-verantwoordelijke die geen deel uit maakt van het managementteam uitgenodigd wanneer ICT-punten op de agenda van het managementteam staan.
Bij de lokale besturen waar de ICT-verantwoordelijke geen rechtstreekse toegang heeft tot het managementteam werd regelmatig aangehaald dat dit het beslissingsproces verstoort of bemoeilijkt (bv. meerdere keren hetzelfde punt agenderen op het managementteam voor een bepaalde beslissing). Gelijkaardige signalen werden genoteerd bij de lokale besturen waar de ICT-verantwoordelijke slechts occasioneel wordt uitgenodigd op het managementteam om ICT-punten toe te lichten.

Daarnaast werd ook nagegaan welke communicatie terugstroomt van het managementteam naar de ICT-functie, vooral wanneer er keuzes gemaakt worden die een impact hebben op de werking van de ICT-functie. Uit de diepte-interviews met de 45 lokale besturen blijkt dat bij een gebrek aan regelmatige communicatie vanuit het managementteam, de continue ondersteuning van de ICT-functie aan de eindgebruikers niet gegarandeerd kan worden. Dit is bijvoorbeeld het geval wanneer de ICT-functie niet tijdig geïnformeerd wordt wanneer een andere dienst een project opzet met een ICT-component. Hierdoor bestaat het risico dat de ICT-functie laattijdig geïnformeerd wordt en/of dat keuzes gemaakt worden die niet compatibel zijn met de ICT-omgeving van het lokaal bestuur en/of die de informatieveiligheid in het gedrang brengen.

In elk van de 45 diepte-interviews uitte de ICT-verantwoordelijke de bezorgdheid dat een goede wisselwerking tussen de ICT-dienst en het managementteam essentieel is om een degelijke ICT-visie/strategie vorm te geven, uit te rollen en om de risico's tijdig te identificeren en onder controle te brengen.

BIJLAGE 1: ALGEMENE INFORMATIE OVER DE THEMA-AUDIT BEHEER VAN ICT-RISICO'S BIJ LOKALE BESTUREN

1. AUDITREIKWIJDTE

Met deze audit over het beheer van ICT-risico's ging Audit Vlaanderen na hoe 144 lokale besturen die voor oktober 2021 geen ICT-veiligheidsaudit besteld hadden omgaan met het beheer van (hun) ICT-risico's.

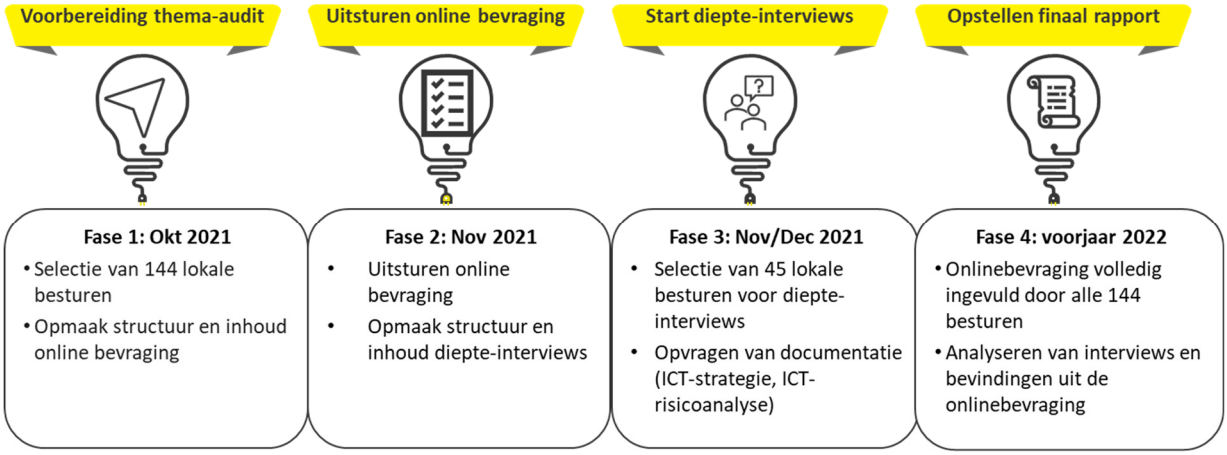
2. AUDITDOELSTELLING

Met deze audit wil Audit Vlaanderen een overkoepelend beeld schetsen van de maturiteit van de lokale besturen op het vlak van het beheer van ICT-risico's.
Als een organisatie actief aan het beheer van haar ICT-risico's doet betekent dit dat er afspraken en governance bestaan en dat er een werkwijze is binnen de organisatie om:

- **duidelijke doelstellingen en visie/strategie te formuleren** op het vlak van digitalisering en ICT-beheer. Deze ICT-visie/strategie houdt rekening met bedreigingen en trends;
- **risico's tijdig te identificeren, te communiceren en** deze ook **te analyseren** via een inschatting van de waarschijnlijkheid van de bedreiging en de mogelijke consequenties of impact voor de organisatiedoelstellingen;
- en de **juiste beheersmaatregelen** (risicorespons) te voorzien.

3. AUDITAANPAK

Deze thema-audit werd uitgevoerd door een team van auditoren van Audit Vlaanderen in samenwerking met Deloitte.
Audit Vlaanderen nodigde oktober 2021 de 144 lokale besturen[2] uit een online vragenlijst in te vullen. Deze vragenlijst bevatte ook een zelfevaluatie over het beheer van ICT-risico's. Vervolgens werden 45 van de 144 lokale besturen geselecteerd voor een diepgaander gesprek met de ICT-verantwoordelijke.



[2] Bijlage 2 bevat een overzicht van de participatie van de lokale besturen aan deze audit.

Vaak namen ook de algemeen directeur, de functionaris voor gegevensbescherming (DPO) en een externe ICT-dienstverlener deel aan het gesprek. Op basis van deze dialoog ontstond een beeld over de manier waarop lokale besturen aan het beheer van ICT-risico's doen en de rol die het management, de interne ICT-functie en ook externe dienstverleners daarbij opnemen. De uitdagingen en struikelblokken maar ook goede praktijken werden tijdens de diepte-interviews in kaart gebracht[3].

Er werden geen audits uitgevoerd bij individuele lokale besturen en er worden dus ook geen specifieke auditrapporten per lokaal bestuur bezorgd.

[3] De selectie van de 45 lokale besturen voor de diepte-interviews gebeurde op basis van volgende criteria:

- hun antwoorden op de online bevraging;
- geografische spreiding;
- het aantal inwoners.

Op basis hiervan werd een zo divers mogelijke groep van 45 lokale besturen geselecteerd.

BIJLAGE 2: DE GEAUDITEERDE BESTUREN

Audit Vlaanderen bevroeg in de periode november 2021-januari 2022 via een online bevraging 144 lokale besturen gespreid over Vlaanderen. Bij 45 van deze lokale besturen werd een diepte-interview afgenomen met de ICT-verantwoordelijke of andere medewerker(s) betrokken bij het beheer van ICT-risico's.
Hieronder een lijst van de lokale besturen per provincie. Bij de lokale besturen aangeduid met (*) werd een diepte-interview afgenomen.

provincie Antwerpen: 30 lokale besturen

- Arendonk (*)
- Baarle-Hertog
- Beerse
- Boechout
- Bonheiden
- Bornem (*)
- Brasschaat (*)
- Brecht
- Duffel
- Edegem (*)
- Grobbendonk (*)
- Heist-op-den-Berg
- Herentals (*)
- Herselt
- Hulshout
- Kapellen
- Lier
- Meerhout
- Nijlen (*)
- Putte (*)
- Puurs-Sint-Amands
- Ranst
- Retie
- Rumst
- Vorselaar (*)
- Vosselaar
- Wijnegem
- Willebroek
- Wommelgem
- Wuustwezel

provincie Limburg: 15 lokale besturen

- As
- Borgloon (*)
- Genk (*)
- Halen (*)
- Herk-de-Stad (*)
- Herstappe
- Hoeselt
- Houthalen-Helchteren (*)
- Kinrooi (*)
- Kortessem (*)
- Lummen
- Maasmechelen
- Tongeren (*)
- Voeren
- Zonhoven

provincie Oost-Vlaanderen: 23 lokale besturen

- Aalter
- Beveren
- Dendermonde (*)
- Evergem
- Gent (*)
- Geraardsbergen
- Haaltert
- Hamme
- Horebeke
- Kaprijke (*)
- Lede
- Lierde (*)
- Maarkedal
- Maldegem
- Melle
- Merelbeke (*)
- Ninove (*)
- Oudenaarde (*)
- Sint-Laureins
- Sint-Lievens-Houtem
- Wichelen (*)
- Zelzate (*)
- Zwalm

provincie Vlaams-Brabant: 39 lokale besturen

- Affligem (*)
- Asse (*)
- Beersel
- Begijnendijk
- Bertem
- Bever
- Bierbeek
- Boortmeerbeek
- Diest
- Dilbeek (*)
- Drogenbos
- Geetbets
- Haacht (*)
- Halle
- Herent
- Holsbeek
- Kampenhout (*)
- Kapelle-op-den-Bos
- Keerbergen
- Kortenberg
- Kraainem
- Lennik
- Linkebeek
- Linter (*)
- Londerzeel (*)
- Lubbeek
- Merchtem
- Opwijk
- Oud-Heverlee
- Pepingen
- Roosdaal (*)
- Sint-Genesius-Rode
- Steenokkerzeel
- Tervuren
- Tielt-Winge (*)
- Wezembeek-Oppem
- Zaventem (*)
- Zemst
- Zoutleeuw (*)

provincie West-Vlaanderen: 37 lokale besturen

- Alveringem
- Ardooie
- Avelgem
- Brugge
- De Haan
- Deerlijk (*)
- Dentergem
- Harelbeke
- Heuvelland
- Hooglede
- Ichtegem
- Jabbeke
- Koekelare
- Kortemark
- Kortrijk
- Langemark-Poelkapelle
- Ledegem
- Lo-Reninge (*)
- Menen (*)
- Mesen (*)
- Middelkerke (*)
- Moorslede
- Nieuwpoort (*)
- Oostende
- Oudenburg
- Pittem
- Poperinge (*)
- Roeselare
- Spiere-Helkijn
- Staden (*)
- Veurne
- Vleteren
- Waregem
- Wielsbeke
- Zonnebeke
- Zuienkerke
- Zwevegem

COLOFON

VERANTWOORDELIJKE UITGEVER
Mark Vandersmissen
Administrateur-generaal Audit Vlaanderen

CONTACT
Audit Vlaanderen
Havenlaan 88, bus 24
1000 Brussel
02 553 45 55

Deze publicatie is beschikbaar op www.auditvlaanderen.be